

CSO

B U S I N E S S R I S K L E A D E R S H I P

Secrets of Your Success

Change management
and business focus

PAGE 26

Scanners Too

Finding network
vulnerabilities

PAGE 18



REAL TIME

**The surprising
security impact of
the simple computer
clock** PAGE 22



SECURITY NOTICE



RESTRICTED
AREA
KEEP OUT

**PRIVATE
PROPERTY**
NO TRESPASSING

There are a number of ways to protect your network.
The first should be to give CDW a call.



Cisco® ASA 5505 Adaptive Security Appliance

- Secures your network against attacks such as worms, viruses, spyware, keyloggers, Trojan horses, rootkits and hackers
- Delivers secure remote access to authenticated users on both managed and unmanaged endpoints
- Combines feature-rich VPN connectivity with comprehensive threat defense to deliver cost-effective remote network access
- Prevents unauthorized access to applications or information assets by providing businesses with fine-grain, identity- or network-based access control



\$414⁹⁹
CDW 1065037



SonicWALL® Network Security Appliance (NSA) 2400

- Utilizes a multi-core hardware design and patented, reassembly-free DPI with 6GbE interfaces
- Delivers real-time network protection without compromising performance
- Offers threat prevention, rapid deployment and lower total cost of ownership
- Combines high-speed intrusion prevention, file and content inspection, and powerful application firewall capabilities with an extensive array of advanced network and configuration flexibility features



\$1936⁹⁹
CDW 1464508



Download FREE trialware at CDW.com/endpoint

Symantec™ Endpoint Protection 11.0

- Includes optimized client and server performance, further scalability controls and virtualization support
- Provides key improvements that build on the stability and efficiency of Symantec Endpoint Protection, enabling comprehensive protection and optimal performance for all environments

100-249 user license with 1-year Essential Support¹ \$32.99 CDW 1314200



We're there with the security solutions you need.

Security threats won't get on your network if they can't get to the network. That's why gateway security is so important. CDW has a wide selection of top-name firewall protection, antivirus, antispyware, intrusion prevention and more. Our personal account managers along with our highly trained technology specialists have the expertise you need to ensure your network is fortified and secure. So call CDW today. And eliminate threats before they even become threats.

CDW.com | 800.399.4CDW



The Right Technology. Right Away.®

¹Essential Support includes 24x7 technical phone support and upgrade insurance; call your CDW account manager for details. Offer subject to CDW's standard terms and conditions of sale, available at CDW.com. ©2009 CDW Corporation

Contents

March 2009 Vol. 8, No. 2

Features...

22 Right on Time?

Cover Story | Forensics Every computer in your company has a clock. Forensics demands precise synchronization. Do you have the time? *By Simson Garfinkel*

26 Plan to Succeed

Physical Security Excerpt: Identifying business goals and driving change are the keys to security strategy. *By Timothy Giles*



Also Inside...

2 From the Editor

4 From the Publisher

6 Join the Discussion
CSOonline readers debate securing Monster.com's website and hacktivism.

9 Briefing

- Social networking dangers exposed
- West Wing BlackBerry security: Possible or pipe dream?
- Downadup worm infects one in 16 PCs
- Data breaches get more costly for businesses
- 5 musts for advancing video surveillance
- Security wisdom watch
- IE or Firefox: Which is more secure?

18 Toolbox

Beating Hackers to the Punch Better to find your network vulnerabilities before attackers do. But how? *By Bob Violino*

30 Undercover

The Company that Did Everything Wrong, Part 2 The conclusion to last month's tale of a comical yet sad visit to a company that suffered a data breach.

34 Industry View

Employee Monitoring: Good for the Employee? ArcSight's CEO argues that "Big Brother" concerns are misplaced. *By Tom Reilly*

36 Debriefing

KFC recipe safe at last



CSO (ISSN 1540-904X) is published monthly except for a combined issue in July/August and December/January by CXO Media Inc., 492 Old Connecticut Path, P.O. Box 9208, Framingham, MA 01701-9208. Periodical Postage Rate at Framingham, MA 01701, and at additional mailing offices. Canadian Publications Mail Agreement number 1902075. **Canadian Postmaster:** Please return undeliverable copy to P.O. Box 1632, Windsor, ON N9A 7C9. Copyright 2008 by CXO Media Inc. All rights reserved. Reproduction of material appearing in CSO is forbidden without written permission. Permission to photocopy for internal or personal use or the internal or personal use of specific clients is granted by CSO for users through the Copyright Clearance Center, provided that a fee of \$3.50 per copy of the article is paid directly to Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01970. www.copyright.com. Please specify: ISSN 1540-904X. Permission to photocopy does not extend to contributed articles—followed by this symbol: †. Address inquiries to CSO, P.O. Box 3482, Northbrook, IL 60065; 866.354.1125. CSO is free to qualified security executives. To all others the one-year basic rate is \$70 for the United States and Canada, \$95 to foreign countries (payable in U.S. funds only). The single copy price is \$9 to the U.S. and Canada and \$15 International. Please allow four to six weeks for new subscriptions to begin. Change of Address: Go to www.amedia.com/custsrv/cso and follow the online instructions. **Postmaster:** Send change of address to: CSO, P.O. Box 3482, Northbrook, IL 60065. Printed in the USA.

[FROM THE EDITOR]

Time to Lead

Back in late 2001, the squeeze was on. The dotcom bubble had popped, and trade magazines (which were unreadably fat with ads just 12 months earlier) were suddenly shedding pages. Which means revenues were plummeting.

That is precisely into that headwind that two colleagues and I, all working on *CIO* magazine at the time, circulated an internal pitch to create a leadership-level security publication. In April 2002, we launched CSOonline.com (here, once again, I curse Central States Health & Life of Omaha, Neb., which owns the cso.com domain). The first print issue of *CSO* magazine shipped in September of that year.

Of course the headwind of 2001 looks like a cooling breeze compared to the overall economic gales of today. And it's always tempting in such storms to batten down the portholes, toss dead weight overboard and generally behave in a reactive manner.

Which is, of course, the wrong reaction.

Security is already too reactive. Every morning we wake up, check the headlines and the bug lists and try to lock down or fix or patch today's problem. Yes, I understand that's always going to be part of the job, but it can't be the whole job.

At this year's CSO Perspectives Conference in Clearwater, Fla., we recognize six recipients of the Compass Awards:

- Russ Cancilla, CSO, Baker Hughes
- Lynda Fleury, CISO, UNUM
- Dan Geer, CISO, In-Q-Tel
- John Martinicky, Director of Global Security, Navistar
- Rich Pethia, Director, CERT
- Robert Rodriguez, Former Special Agent, United States Secret Service

The Compass Awards recognize outstanding leadership achievements in the security world. Specifically, this is a crop of people who keep an eye on the horizon instead of the rear-view mirror. They've demonstrated this by creating programs to increase industrywide information sharing, companywide security branding, and everything in between.

Happily, this year's selection process was the most difficult yet. We received the largest number of nominations in the six years that we've conducted the awards process, and could surely have recognized another half-dozen winners. (But there's always next year for that.)



The reason I say "happily" is that it's encouraging to see so many security leaders who focus on business value, who innovate, who lead.

Because in a recession, these qualities are more critical than ever. Now's the time to innovate; now's the time to lead.

-Derek Slater, dslater@cxo.com

CSO

Editor in Chief Derek Slater

Senior Editors

Bill Brenner, Joan Goodchild

Copy Editor

Kristin Burnham

Editorial Administrator

Simone Levien

Contributors

Jarina D'Auria, Simson Garfinkle,
Timothy Giles, Tom Reilly, Bob Violino

DESIGN

Executive Director, Art and Design

Mary Lester

Art Director Steve Traynor

RESEARCH

Research Manager Carolyn Johnson

CXO MEDIA/IDG

COO Matt Smith

CSO Robert Hayes

TECHNICAL ADVISORY BOARD

Jason Cowling

Jeremiah Grossman, WhiteHat Security

Frank Murphy, TBG Security

Stephen Northcutt, SANS Institute

Richard Power, Carnegie Mellon CyLab

EDITORIAL/ADVERTISING/

BUSINESS OFFICES

492 Old Connecticut Path,

P.O. Box 9208,

Framingham, MA 01701-9208

Main phone number: 508 872-0080



INTERNATIONAL DATA GROUP

Chairman of the Board

Patrick J. McGovern

IDG COMMUNICATIONS, INC.

CEO

Bob Carrigan



We protect your data. And your dollar.

Past

- Company goes public
- Upgrade network and backup storage
- Hire new IT Director and Compliance Director
- Expand operations
- Market conditions hurt revenue growth

Present

+ Budgets tighten across the board

- Engage Lumension for security solution
- Reduce IT and security TCO
- Data and network protected
- Meet industry compliance audit

Future

- Positioned for economic turnaround

Reduce Risk. Not Revenue.



Download our white paper on Reducing Security TCO at
www.lumension.com/security-tip-21

1.888.725.7828

Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance



[FROM THE PUBLISHER]

All Security is Local

I was having a discussion with a friend the other day about some political issue or another (I lean a little to the right—all right, a lot to the right, she leans a little to the left...in all things there is balance). I kept focusing my argument on the impact of this issue at a national level and all the problems that come from it. She, on the other hand, kept talking about how it all boiled down to how the average person was affected. "At the end of the day, all politics is local. The big picture is nice, but all anyone really cares about is what it means to them," she said.

As I thought about it, it struck me that security functions in a very similar way. Security isn't always about solving the world's biggest problems. Most of the time it is just about the blocking and tackling. The problem is that we often lose sight of that fact when trying to put out all the forest fires that flare up on a daily basis. As we try to be compliant with this law or that regulation, it's easy to forget that, at the most basic level, simple, proven security efforts can be implemented to defend most of what we need to have defended.

Over the past month I have been having discussions with a number of CSO's readers about how they protect their valuable data. I've heard stories of layered defenses and emerging technologies, complex data classification schemas, "defense in depth," complex rules that apply risk metrics to data evaluation. But increasingly I am hearing that some of you have, to a certain extent, given up on all that and decided that all your data is critical and needs to be secured. The theory being that it's easier to apply policy across everything than to try and split the atom by determining the different levels of data importance and what rules should be applied to each.

In many ways, this is like the political conversation I had with my friend. There is a certain appeal to a complex, tiered solution that addresses a wide range of needs, and often our first tendency (my first tendency at least) is to go for the complex, technical solution. But at the end of the day, isn't it just easier to boil it down to what it means to your organization? It's not really about applying different solutions to address every nuanced regulation and requirement out there or that may be coming. That thinking is what got most of our organizations into the situation they are currently in, with layers upon layers of technologies and policies, each designed to address a specific pain point. To your employees and investors, it's all about making sure that the business continues to operate and that nothing can get



in the way of that. Embrace that, and you may find your job getting a little easier... or at least less complex.

Best regards,
-Bob Bragdon, bbragdon@cxo.com

CSO

President and CEO
Michael Friedenberg
Publisher Bob Bragdon
Senior Ad Sales Associate
Christine McKay
East Coast Regional Manager
Roz Burke
Regional Sales Manager Matt Knuth

INTEGRATED MEDIA AND ONLINE SALES

Vice President, Online Sales
Brian Glynn
Online Regional Sales Manager
Richard Hartman
Online Regional Sales Manager,
West Coast Erika Karr
Manager, Online Account Services
Danielle Tetreault
Online Account Services Specialists
Jennifer Malkasian, Tara Shea
Online Advertising Specialist
Barbara Sullivan

CUSTOM SOLUTIONS GROUP

Vice President Matt Avery
National Sales Director
Adam Dennison

PRODUCTION

VP/Manufacturing Chris Cuoco
Production Manager Heidi Broadley
Associate Production Manager
Lisa M. Stevenson

EXECUTIVE PROGRAMS

VP, Executive Programs
Ellen Daly
Director, Event Marketing
Mary Conroy
Director, Event Operations
Deb Begreen
Editorial Manager Lufe Low
National Sales Manager
Per Melker
Sales Associate
Lauren Costello
Event Planner Sarah Reagan
Event Planner/Client Relations
Laura Biringer
Registration Specialist Cress O'Brien
Marketing Specialist Kristin Gallo
Client Services Specialist Erica Foster

LIST SERVICES

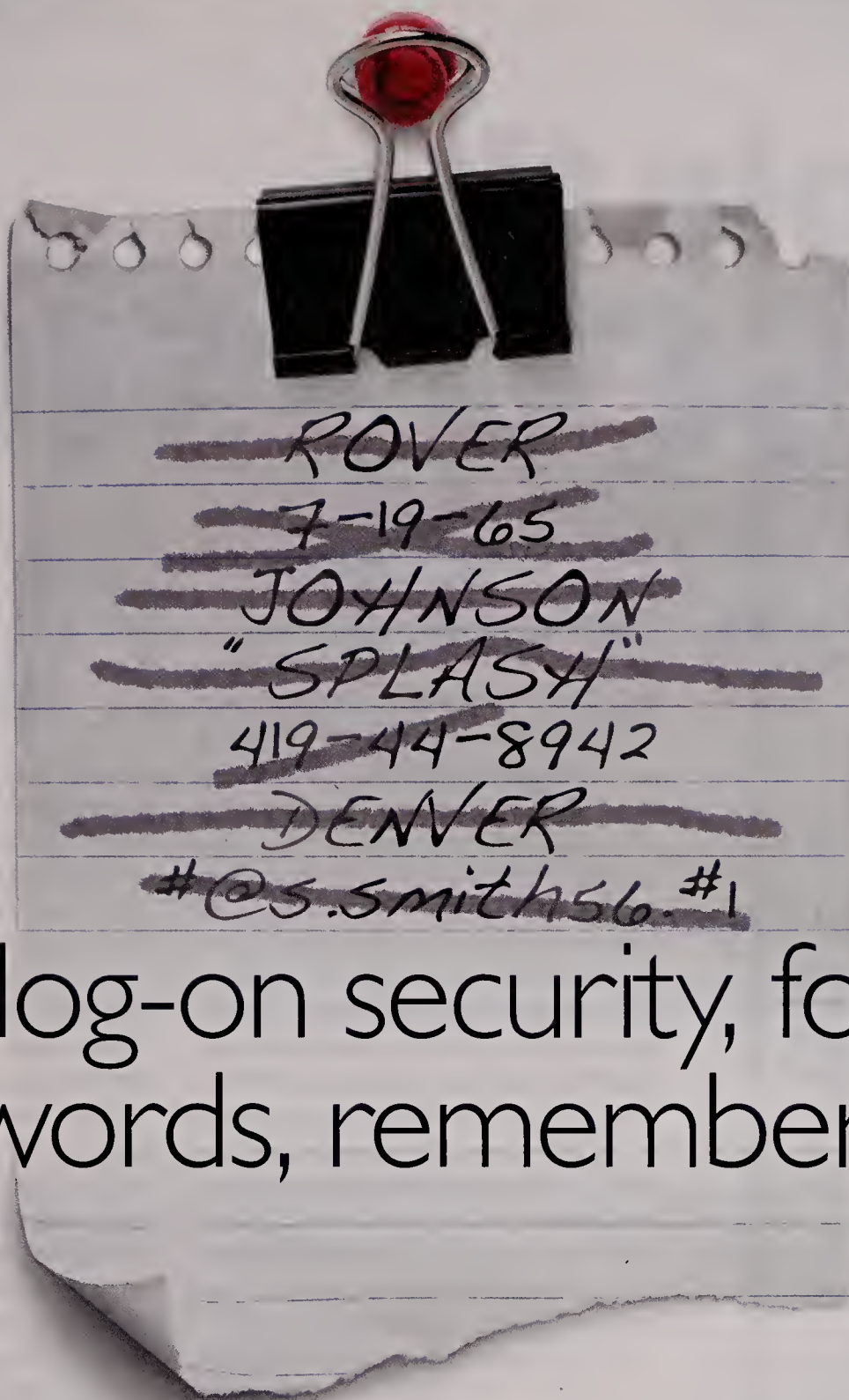
Contact Paul Capone of
IDG List Services at 508 370-0865 or
pcapone@idglist.com

REPRINTS & PERMISSIONS

For information about reprints and
copyright permissions, please contact
The YGS Group, 800-290-5460 ext. 150,
cso@theygsgroup.com

Advertiser Index

CA..... C4	Gemalto 11	RSA Conference 2009 21
CDW Corp. C2	HID Corp. 5	RSA Security 15, 17, 33
CXO Media Inc. 35	ISACA 8	Tenable Network Security C3
Fortify Software 31	Lumension Security 3	Websense Inc. 19
	Ounce Labs 13	



For log-on security, forget passwords, remember HID.

hidglobal.com

HID, the world leader in physical access control can now provide secure access to your network. All on your current card.

Passwords have long been used as a means of log-on security, but an easier, more reliable way to control access to Windows® is the same way you do with your doors – with HID contactless technology.

You don't have to re-badge. It's ready to go from day one with the same credential.

And it's an easy transition for cardholders because they're already familiar with the contactless technology. Proven, cost-effective, simple – HID is where convenience meets security on the desktop.

Get your FREE white paper at passwords.hidglobal.com



ACCESS logic.

Visit HID Global at ISC West, Booth #11052

Join the DISCUSSION

What's on your mind? Security leaders discuss and debate at www.csoonline.com

PRIVACY

Bardin: Maybe This Monster Should Scare Off Attackers

Back on August 31, 2007, I hammered Monster.com on their first reported breach. In their messaging to customers and users alike, Monster indicated that:

"We also have announced a series of initiatives we are taking to enhance security controls for our website. These initiatives are part of the infrastructure improvements that were announced by Monster before the recently reported attack. The initiatives include:

- Implementing new, robust capabilities for worldwide monitoring and surveillance of site traffic;
- Reviewing and tightening all site access policies and controls;
- Launching a series of targeted initiatives to protect job seeker contact information."

This is where Sal Iannuzzi was so kind as to provide his handwritten signature as an attachable image in the messaging that came as an e-mail. Since that time, Sal hired some new people to shore up security and passed the crisis communications to Patrick Manzo, the senior VP, global chief privacy officer.

Patrick indicates that:

"The protection of your data is a high

priority for Monster. Our newly redesigned website has, and will continue to, add safety and security features to protect your information, and we want you to feel confident using it.

"We continue to devote significant resources to ensure Monster has appropriate security controls in place to protect our infrastructure, and while no company can completely prevent unauthorized access to data, Monster believes that by reaching out to job seekers, the company can help users better defend themselves against similar attacks."

Do we really believe that no company can completely prevent unauthorized access to data from occurring?

It would be interesting to compare spending on Super Bowl Sunday advertising to how much money it would take to secure Monster's website or to merely

encrypt user passwords in its database. Not encrypted you ask? Well, if you the hackers stole user IDs and passwords, and Monster wants all users to reset their passwords, I would strongly believe that they were stored in the clear in its database. How many users use the same password on multiple sites? Keep in mind that the cost of the airtime does not include all costs to produce and create the ad.

If you can spend millions on a TV spot, how many thousands of dollars does it take to encrypt the password field? Is it even in the thousands? What did it cost to make-over this fine vehicle?

In light of how this year is starting off with respect to data breaches, I'm not getting a warm and fuzzy



MORE ON THE WEB

Social Engineering: Anatomy of a Hack

"Cookies are the keys to everyone's heart. **I started passing out cookies to everyone.** We were all laughing, having a great time. Meanwhile, we were in the middle of hacking their entire network."

www.csoonline.com/article/479038

feeling that my personal wall of shame (the wall where I collect and show off the letters I've received from companies who have lost my data) will not need more space.

-Jeff Bardin

HACKING

Olzak: Are You Vulnerable to Hacktivism?

Through the years, activism has taken many forms. Marches, picketing, egg throwing, billboards and sit-ins have been used to drive home a point, to change the behavior of governments, corporations or societies. In developed nations, these activities were historically localized with limited impact on infrastructure, the economy or whether a corporation continued to operate. Technology has changed all that.

Today's activists, through the use of the Internet and other computing technology, have the ability to cause serious or irreparable harm to governments, politicians, executives or corporations targeted by their agendas. The joining of computer hacking and activism falls under the single handle of "hacktivism."

Alexandra Whitney Samuel defines hacktivism as "the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools, according to Samuel's 2004 thesis, "Hacktivism and the Future of Political Participation," include website defacements, redirects, denial-of-service attacks, information theft, website parodies, virtual sit-ins, virtual sabotage and software development.

Political hacktivism—although some still believe it was nationally sponsored hacking—was seen in the virtual attack on Estonia in 2007. More recently, Georgia and Kyrgyzstan experienced attacks against their infrastructure. In addition to country-level attacks, numerous high-profile organizations and individuals have also experienced hacktivism in the form of website defacement or the release of sensitive or embarrassing information. Here are

some examples:

- Microsoft's Irish website defaced;
- Scotland Yard careers website defaced;
- Hackers defaced collider site, say reports;
- IDC website defaced by 'eco-terrorists';
- Obama website hacked: Users redirected to Clinton campaign website;
- Safe website let you embarrass people in high places;
- Palin's Yahoo mail hacked, published on wikileaks.org.

As security managers, we spend a lot of time protecting the confidentiality of our PII and PHI/ePHI. We lock down access to protect the integrity of financial information. This protects us from financially motivated attackers. But hacktivists have a different reason for stealing information or disrupting your business. The hacktivist wants to turn public opinion against the target or cripple its ability to operate normally.

Browsing wikileaks.org, you can view a wide variety of documents retrieved by unauthorized personnel or provided by disgruntled employees. Once the documents hit the Internet, there is no pulling them back. Even information taken out of context and subjected to spin will float around the Net for years as the target entity tries desperately to deny its authenticity.

Blackmail and extortion are other methods sometimes used when a hacktivist obtains sensitive information about an organization's activities, future plans, etc. "The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications," published in 2000 by the NCS, also noted that instead of asking for cash, the hacktivist might use the information as leverage to block one or more planned objectives.

All these issues add up to a need to protect any information, whether controlled by government regulation or not, which might embarrass or cause operational interruptions if in the wrong hands.

Do your executives document strategy meetings and store the information on their laptops or company servers? Do managers communicate via e-mail about how they feel about union activities? Is your company developing a product or service that might be socially explosive if not rolled out in a controlled manner? Does

HOW TO REACH US

You can contact us directly or post your thoughts on specific articles and blogs at www.CSOonline.com.

Derek Slater, Editor in Chief
dslater@cxo.com
508 935-4213

Bill Brenner, Senior Editor
bbrenner@cxo.com
508 988-7587

Joan Goodchild, Senior Editor
jgoodchild@cxo.com
508 988-7994

Subscriber Services
Phone: 866 354-1125
Fax: 847 564-9453
E-mail: cso@omeda.com

Reprints & Permissions
For information about reprints and copyright permissions, please contact The YGS Group, 800 290-5460, ext. 150, cso@theygsgroup.com.

your organization prefer not to err on the side of transparency in its dealings with the public, a transparency it can point to when the spin doctors accuse it of secret and unethical activities?

The same controls—administrative, physical and technical—put in place to comply with GLBA, SOX, HIPAA or Facta should be expanded to include potentially damaging information as well as public-facing systems (e.g., websites). The process starts with understanding what information, taken alone or when combined with other pieces of data, can be used to further the agendas of those opposed to our business or political outcomes.

-Tom Olzak

INVENT YOUR FUTURE.

Get Certified!



Exam Registration Deadline: 8 April 2009

Exam Date: 13 June 2009

CISA
CERTIFIED INFORMATION SYSTEMS AUDITOR™

CISM
CERTIFIED INFORMATION
SECURITY MANAGER®

CGEIT™
CERTIFIED IN THE GOVERNANCE
OF ENTERPRISE IT™

Visit www.isaca.org/csomag.

ISACA®
Serving IT Governance Professionals



"Even if you put the privacy settings in place, you should assume you are screwed." (SEE BELOW)

Briefing

TRENDS, STATS AND FAST FACTS

Edited by Bill Brenner

Slapped in the Facebook: Social Networking Dangers Exposed

Two security researchers demonstrate the many ways that bad people can tamper with your Facebook account, MySpace page or LinkedIn profile

For many people, social networking has become as much of a daily routine as brewing coffee and brushing teeth.

IT administrators dislike it.

Cyber crooks depend on it.

That's because much of the time that people spend on MySpace, Facebook, LinkedIn, Twitter and elsewhere is during work hours—on work machines.

At the ShmooCon 2009 security conference in the nation's capital last month, two security researchers demonstrated the many reasons why this is bad.

In a presentation called "Fail 2.0: Further Musings on Attacking Social Networks," Nathan Hamiel and Shawn Moyer guided attendees through attacks made easy because of the very nature of these sites, where users can upload and exchange pictures, text, music and other content with little effort.

"Social networking sites are meant to get as many users in one place as possible on one platform, and for attackers, there's a lot of return-on-investment in going after them," Moyer said, describing the climate as a perfect storm of social engineering and bad programming.

Through a variety of easy tricks, attackers can hijack a person's social network account to use as a launching pad for additional attacks against other users, other Web 2.0-based

applications and so on.

Social networks can also be incorporated into micro botnets and, by rummaging through a page of misfired direct messages on Twitter, a motivated attacker can unearth the cell phone numbers of prominent people.

Hamiel noted that the trouble begins with so much creative power being put in the hands of those who have little or no tech savvy.

"Any application can be used to attack other applications and an application can be used to view your entire file if the privacy settings are off," he said.

"Even if you put the privacy settings in place, you should assume you are screwed."

The demonstrations the duo ran through included:

- Creating imposter profiles on LinkedIn, assuming the identity of someone prominent and friending as many people as possible;
- For the sake of experimentation, the researchers created a fake profile for a well-known security leader (with permission) and accumulated 50-plus connections in less than a day, many of them CSOs and other bigwigs;
- Showing how to sabotage the MySpace page of someone you're not directly connected with via the profile of a common connection; (This example involved fake MySpace pages for rocker Alice Cooper and actors Eva Longoria and Bob Saget.

In this scenario, Cooper and Longoria are connected to Saget but not to each other.



Longoria wants to connect with Cooper, who refuses, and she responds by using their common connection to Saget to access and deface Cooper's page.)

- Rummaging through a site that accumulates old direct messages originally sent out through Twitter.

With enough patience, the bad guy can find and exploit such discoveries as phone numbers, e-mail addresses and other personal information that was originally meant for individuals rather than the general Tweeting public.

Not surprised by any of this is James Arlen, a Toronto-based security consultant who listened in on the presentation.

"At the end of the day, far too many people operate in a zone where they presume trust," Arlen said. "There's an odd level of trust where you look at someone's profile and say 'I know this person,' but there's no real attempt at authentication."

-Bill Brenner



>> BRIEFING

Q&A

West Wing BlackBerry Security: Possible or Pipe Dream?

Former White House Deputy Chief of Staff Joe Hagin is the guy who planned George W. Bush's secret trips to Iraq and Afghanistan and oversaw renovations to the Situation Room and press briefing room. He was also the one in charge of securing every BlackBerry used in the West Wing. In this Q&A, he opines on Obama's BlackBerry use and the security measures every smart phone user should heed.

Talk about some of the pros and cons of BlackBerry use in the West Wing from a security perspective.

Joe Hagin: When we first got to the White House, there were no BlackBerries, there were no smartphones in the executive branch. The folks on Capitol Hill began using BlackBerry technology and it proliferated very rapidly up there. On Sept. 11, 2001, when we had so much trouble in the executive branch communicating during the emergency, when commercial phones and cell phones went down to a large extent because the system overloaded, there was a lot of difficulty at the White House because the president was in Florida, I was in New York City and everyone else was in Washington, D.C. With everyone spread so thinly, we had trouble figuring out who was OK, the status of things and so on. In the weeks that

followed, when talking to some of our friends on the hill, we found that they had stayed in pretty good touch through BlackBerry technology. We ultimately decided to proceed with a limited distribution of BlackBerries in the White House. It started with 50, turned to 200 and today I think almost everyone there is using one.

What were the security restrictions you established?

We banned classified material from any over-the-air device that was not encrypted and approved by various federal agencies. Both the sending and receiving party would have to have one of the secure devices. The problem facing the president is not much different from what business leaders face. The business leaders just aren't as aware of the risks.

We know President George W. Bush refrained from e-mail during his two terms, but did he ever lament on how he really wanted a BlackBerry? Or was he leery of the security straightaway?

Well, he was a prolific e-mailer as Texas

governor and he really didn't want to give that up as president. But when faced with the barrage of briefings from White House lawyers and security personnel, he accepted the no e-mail creed. It's the same kind of pressure I'm sure President Obama has just gone through.

But Obama stood his ground and didn't give up his BlackBerry.

I'm not privy to what they have done technologically, and I know there's speculation that it's a secure BlackBerry. But if that's the case, all his friends have to be e-mailing him from equally secure BlackBerries. From what I see in the news, it doesn't look like a secure BlackBerry because the secure devices tend to be much thicker than the state-of-the-art variety. But it's hard to comment without being certain of what exactly they've put on his device to restrict and protect it. In terms of limiting the number of people who have the address, well, you know how hard it is to keep an e-mail address secret. And getting an e-mail from the president is a heady thing, so we'll see how long they can keep it secret. -B.B.

BY THE NUMBERS

\$202

Cost for every compromised customer record, according to the Ponemon Institute

46%

Increase in data breach cost compared to last year's Ponemon study

100M

Number of records potentially compromised in a security breach at Heartland Payment Systems

1 in 16

Number of PCs thought to be infected by the Downadup worm

How can I keep
my passwords
safe? _

justaskgemalto.com



For quick and practical answers to your digital security
questions when communicating, buying, traveling and surfing,
there's only one place to go: www.justaskgemalto.com

Enjoy your digital life.

gemalto
security to be free

Downadup Worm Infects One in 16 PCs

Scans show six percent of PCs already hit with worm; figure may be as high as 30 percent

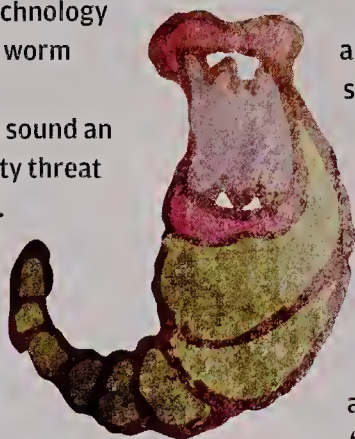
The computer worm responsible for the biggest attack in years has infected at least one out of every 16 PCs worldwide, and it may have managed to compromise as many as nearly one in three.

According to Panda Security, almost six percent of the Windows systems scanned with its antivirus technology were found to be infected with "Downadup," a worm that began aggressive attacks in January.

Panda was one of the first security firms to sound an alarm over Downadup when it raised its security threat level on Jan. 12, as reports of attacks mounted.

Using data from antivirus scans performed by its consumer-grade security software and by a free online scanning tool that it makes available on its website, Panda found 111,379 PCs infected with the worm out of a pool of two million machines.

"I'm pretty confident in this number," says Ryan Sherstobitoff, chief corporate evangelist at Panda Security, as he cautioned it was just a snapshot. "Conficker is still infecting high volumes of machines and is a fast-propagating worm."



Conficker is an alternate name for the Downadup worm.

In fact, Panda's estimate is probably very conservative, Sherstobitoff says, since the bulk of the infected computers were scanned when their owners took the time to steer their browsers to the company's online scanner.

"The six percent was of people coming to our site and opting in for the scans. That's somewhat scary," says Sherstobitoff. "If we were actually to look at the [general] population, all the people who don't have antivirus—or if they do, who haven't updated definitions—the infection rate might be in the range of 20 percent to 30 percent."

While there has been some disagreement among security researchers about Downadup's infection volume, there has been little argument about the relative size of the worm attack.

"This is the biggest in at least six years," says Sherstobitoff. And things will get worse before they get better. "This is an epidemic, and the worst may still be to come as the worm could begin to download more malware onto computers or to spread through other channels," Corrons says. —Gregg Keizer

METRICS

Data Breaches Get More Costly for Businesses

Companies that are reluctant to invest what it takes on data security better be prepared to pony up a lot more if their systems are ever breached.

That's the main takeaway from a new report released by the Ponemon Institute, which shows that the average cost of a data breach to companies is continuing to increase.

Ponemon said the breaches from last year that it studied cost an average of about \$202 for each compromised customer record.

That is 46 percent higher than the \$138 per record that Ponemon cited in its first

annual report on breach costs, for 2005.

The average cost had previously increased to \$182 in 2006 and \$197 in 2007, according to Ponemon.

The cost-per-record figures include direct expenses for breach detection, mitigation, notification and response efforts, as well as indirect costs, such as the financial impact of customer defections and lost business opportunities.

Ponemon said the average overall cost of the breaches covered in the new report was more than \$6.6 million, with individual companies reporting costs that ranged from \$613,000 to almost \$32 million.

The report was based on a study of breaches at 43 large companies from 17 different industries. The number of customer records that were compromised in the breaches ranged from less than 4,200 to more than 113,000.

Those figures are much lower than those associated with the most-publicized

breaches, which involve compromised records numbering in the millions, but they're in line with the number of compromised records involved in the types of breaches that typically hit companies. Increasingly, the biggest cost to companies that suffer data breaches is lost business, says Larry Ponemon, chairman of the Elk Rapids, Mich.-based think tank.

He adds that about \$139 of the average per-record breach cost, or 69 percent of the total, was in the form of lost business last year, while other costs declined.

That statistic indicates that although companies are getting better at detecting and responding to data breaches, customers are becoming less tolerant of breaches and showing a growing willingness to take their business elsewhere, Ponemon said.

In the wake of breach reports, "we found customer churn rates actually going up," Ponemon said. "People do care deeply about data being stolen." —Jaikumar Vijayan



Ensuring Application Security

Knowledge is power in risk-averse software development environments

Jack Danahy, CO-FOUNDER AND CTO, OUNCE LABS

Danahy is a prominent advocate of application security, a patent holder in multiple security disciplines, the founder of two successful security software firms, and a frequent speaker and writer on topics of national and industrial cyber security.

Application software is ubiquitous, whether it's for cell phones, cameras, automobiles or nuclear submarines. All these devices rely on application software to run their systems, and all of them need to be secure. As organizations begin to realize the dangers of insecure software applications, they are increasingly adapting measures to protect their systems.

Why has cyber crime increased so dramatically in recent months?

The recent increase in cyber crime incidents is mainly due to two things: there is an increased awareness of these events.

"The biggest risk is lack of communication. There is danger if I assume that my outsourced applications will be properly secure."

The new data breach disclosure laws and the new ways organizations react to data loss means that we're learning more about breaches than we used to. The second reason is there is a lot more information to go get. There is an entire underground economy that deals and trades in the private information that gets stolen, and the presence of that means there is more reason to break into systems.

How big is the application security risk to businesses?

In my opinion, the risk is enormous. Almost everything an organization does with data—whether it's the way they deploy

their plans, the way they deal with their partners and customers, or the way they manage their own financials—is controlled by software applications. And since we have never looked at an application that didn't have a flaw in it during the seven years we have been in business, it strikes me that if such a critical component of your infrastructure is virtually always vulnerable, that component introduces an enormous amount of risk.

How aware are users of this risk?

I think there is a certain lack of awareness about how vulnerable many of these ap-

plications can be; people are fearful that simply looking into this area of risk creates an intractable problem. They don't recognize that they can take steps to make it better without getting buried in the amount of data they're going to find.

Where should companies start to focus to effectively combat the threat?

We talk to people who are just beginning this process and ask them how many applications they have. Many of them don't know, let alone have any insight into what those applications do or what kind of information they're handling. That being the case, my first step for all these organiza-

tions—before they buy any product, even ours—is to understand how many applications they have, what those applications are doing, and what kind of data and services those applications are serving up.

What additional security risks are associated with outsourced applications?

The biggest risk is a lack of communication. There is danger if I assume—without ensuring—that my outsourced application will be properly secure, because the outsourcer may build an otherwise good application that is lacking some fundamental security component that I did not rigorously specify. There is also an enormous amount of outsourcing with cloud computing, which outsources the delivery of the application service as opposed to the code itself. This has to be tightly examined or the service you're offering ends up as a black box, and that's never a good idea where private information and security are concerned.

FOR MORE INFORMATION:

Check out the white paper titled "5 Steps to Starting Application Security" at www.csoonline.com/whitepapers/ouncelabs.

 **OUNCE LABS**

CSO
Custom Solutions Group



5 Musts for Advancing Video Surveillance

Video surveillance was once the exclusive province of physical security; operators looked at multiple video screens, each displaying the field of view of a single video camera, to monitor for security incidents. But increasingly, the charge of fully securing an organization's assets requires a larger number of cameras with multiple viewers of the video information.

As these systems add more video to be watched, there becomes a need to use IT style analysis tools to help sort through the myriad incoming video to find potential threats. With that, CSOs find themselves required to integrate a key physical security solution—video surveillance—into overall IT security.

Here are the top-five criteria to consider when evaluating a video surveillance solution.

1. MOVE FROM ALGORITHMS TO LEARNING. It has proven challenging in video surveillance systems to program a rule for every single unusual activity, but as a natural next step, organizations will require a system that works similarly to current products currently in use in IT departments to detect abnormality in network data streams. Organizations may find the move from algorithmic and rules-based systems to a learning technology a helpful next step to improve a video surveillance system.

2. SCALABILITY IS KEY TO SUCCESS. A video analytics technology capable of learning relies on computing power, which requires organizations to ensure that all elements of the system have the potential to scale to meet the needs of even larger video surveillance operations. Scalability is crucial; the sheer amount of video surveillance now being deployed is staggering.

3. COMPATIBILITY FOR MULTIPLE VIDEO TECHNOLOGIES. Once the video streams are concentrated or stored, what happens next? A level of compatibility is required if the video analytics solutions need to transmit video streams to an analytic engine so that different types of applications can

consume and process the video.

4. DIGITIZED VIDEO AND SECURITY. Today, a full video infrastructure includes cameras, viewing stations, video storage and recall, video analytics and analytic processing. It may include remote monitoring or publishing video to remote locations and it may require encryption of the video stream. Video isn't just video any more. Video is data; data that enters the realm of IT. Like any other type of data, digitized video must be analyzed, shared, transferred, archived, searched and more. This makes it even more crucial for video surveillance systems to comply with open standards, since they are essential to getting the most value from the data.

5. JOINT STANDARDS EFFORTS. Vendors and standards bodies are just beginning to look at enacting guidelines for how to plug different parts of different technologies together: how data will be transmitted, how video streams will be encoded and so on. True interoperability, however, is usually not achieved via vendor-driven organizations. Interoperable, large-scale video surveillance solutions will only be achieved with the participation of end-user organizations.

—Eric Eaton is CTO of BRS Labs

SECURITY WISDOM WATCH

A look at some of the finer (or not so fine) moments in the last month



Thumbs both ways: Kaspersky Lab. The vendor was pretty open about its recently suffered data security breach, quickly admitting it never should have hap-

pened. But when you're a security vendor, most people are still going to wonder how you ever let it happen in the first place.



Thumbs down: Facebook.

The bad guys are finding it's very easy to dupe people out of their hard-earned reputations on the popular

social networking site. Example: Facebook's discovery that the bad guys are establishing dummy profiles to extract credit card numbers and other data from well-meaning Facebook "friends."



Thumbs up: Wolfgang

Kandek. The chief technical officer at security company Qualys made a suggestion that Microsoft would do well

to heed—severing Internet Explorer from the rest of Windows and making it a standalone application that can be patched more frequently and easily like Firefox.



Thumbs up: Patch Tuesday.

Despite recent zero-day attacks against Microsoft's products and suggestions that patches should be released more frequently, most IT admins interviewed by CSO say that Patch Tuesday is much better than the old way that fixes were released.



Thumbs up: Security Twits.

This group of security pros is proving the value of Twitter as a place to debate and solve security problems. —B.B.

Verbatim...

"Even if you put the privacy settings in place, you should assume you are screwed."

-Security Researcher Nathan Hamiel, regarding the flakiness of privacy settings in such portals as LinkedIn, Facebook and MySpace

"I have always thought of Patch Tuesday as a great attack vector for evil-doers. If you know when patches are released and (should be) applied, you have one more variable in your arsenal of tools."

-Kurt Baumgarten, a Boston-based information security executive, taking the opposite view of Patch Tuesday

"Social networking sites are meant to get as many users in one place as possible on one platform, and for attackers, there's a lot of return-on-investment in going after them."

-Hacker Shawn Moyer, during the ShmooCon security conference in Washington, D.C., last month

"There's no more last-minute rush to hold an IT staff onsite to make an emergency patch install on an unknown day. No more worrying about having time to schedule testing and so on."

-Paul Robertson, a Washington D.C.-based network security specialist and computer forensics examiner, on why Microsoft's Patch Tuesday cycle has been helpful to IT shops

**Data loss prevention is your priority #1.
Shouldn't your security vendor rank just as high?**





BROWSER SECURITY

IE or Firefox: Which Is More Secure?

The conventional wisdom in security circles used to be that Microsoft's Internet Explorer was hopelessly attack-prone and that only someone with a cyber death wish would prefer it over such alternatives as Mozilla Firefox, Opera or Apple's Safari browser.

That is, no doubt, still the case for some. But with Microsoft more focused on IE security than it used to be, and with the market increasingly saturated with Web-browsing alternatives like Google Chrome, opinions aren't as sharp as they once were.

CSO recently conducted a highly unscientific, very informal poll of security practitioners, asking which browser they consider more secure.

Firefox still scores well for many who like the frequent and easy security updates. But IE seems to be gaining more acceptance, especially since Microsoft released version 7 a couple of years ago. In the final analysis, though, security pros say that the quality of one's IT defenses can't be based on the browser a company uses.

If one were to get into a flaw count between browsers, the security of each would rate about the same.

With attacks increasingly aimed at the application layer, and Web apps a particularly juicy target, it's clearly critical that all browser-makers continue to improve.

However, security pros say that from their point of view, it's better to worry less about the browser and more about what other security layers are in place throughout the organization.

Favoring Firefox

When Mozilla launched Firefox 1.0 in late 2004, users praised it as the ironclad alternative to IE, whose security reputation was at a low point after years of withering attacks targeting a cornucopia of vulnerabilities.

Some began questioning the security of Firefox after a steady stream of security fixes that rivaled the number usually found in a Microsoft Patch Tuesday release. But its popularity remains largely undiminished among the security crowd.

Asked for his preference, Chicago-based critical infrastructure

researcher and security author Bob Radvanovsky didn't hesitate:

"Firefox, without a doubt," he said. "Something that doesn't record my keystrokes or keep my cached information, and does what I ask it to do."

Tudor Panaitescu, manager of global network security at Colorcon in the Philadelphia area, says Firefox has been key to his efforts to be Windows-free.

"I use Firefox on Linux 99.9 percent of the time. I have to admit that for the last couple of years, I am Windows-free; no Windows on my workstation at work nor on my PCs at home," he says.

IE Better, But Still Flawed

IE still has many security holes, and Microsoft's monthly patch updates almost always include a cumulative update for the browser.

But the mere mention of IE doesn't cause the chorus of sneers and groans that was typical half a decade ago. That doesn't mean security pros now embrace it unconditionally.

"I use IE 7, but I must confess this is not a security choice but a compatibility one," says François Amigorena, president and CEO of French security software company IS Decisions. "As an Independent software vendor specializing in security solutions for Windows-based infrastructures, my company uses a bunch of Microsoft products, including Exchange, SQL Server, Dynamics CRM, SharePoint, Groove, Live Meeting and so on."

Others are more indifferent about which browser they use. It's not that they don't care, it's that they feel about the same level of security with the likes of IE and Firefox.

One IT security professional who requested anonymity says that he uses both and makes sure each are kept up to date on the security patches.

He also uses a secure hardware device from IronKey to store his online passwords so when he needs to use someone else's PC, he can launch the browser from the secure memory on his USB key.

-B.B.

Ranked #1 out of 100 vendors
(CIO Insight, 12/08).

1000+ technology
integration partners.

Chosen by 3/4 of
the Fortune 100.

For unmatched protection of your sensitive enterprise data:

Find security in RSA.

www.rsa.com



The Security Division of EMC

Security Information and Event Management | Data Loss Prevention | Identity & Access Management

©2009 RSA Security Inc. All rights reserved. RSA and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and other countries.

Toolbox

TOOLS, TECHNOLOGIES AND TACTICS

By Bob Violino

Beating Hackers to the Punch

Better to find your network vulnerabilities before attackers do. But how?

As any network and security manager knows, new vulnerabilities are constantly being discovered and threats against corporate networks are getting increasingly sophisticated.

Proactively scanning for vulnerabilities can help identify weaknesses before they become damaging to enterprise IT environments.

Vulnerability scanners are software products that regularly analyze networks and network devices and then present results to users in reports that enable them to respond quickly to problems.

Network-based scanners look for vulnerabilities such as firewalls that have been configured incorrectly or servers that might be susceptible to Web-based threats.

"At the 100,000-foot level, most network vulnerability scanners do pretty much the same thing: scan networks of computers, either externally or internally, to determine what hosts are running on the network and the characteristics of those hosts," such as IP address, operating system and applications that are running, says Paul Roberts, senior analyst in the Enterprise Security Practice at The 451 Group. Scanners accomplish this by sending out network traffic in a variety of formats, Roberts says. "For example, simple PING trace features, which send out ICMP (Internet Control Message Proto-



col) echo request packets, might be used to determine just what hosts are on a network [or] which IP addresses in the IP address space used by the company are taken," he says. "Once hosts have been profiled, they can be probed for known vulnerabilities, configuration issues and so on."

Newer features include the ability to support enterprisewide, distributed scanning and to manage that centrally, says Chenxi Wang, principal analyst at Forrester Research. Also emerging is the ability to support some kind of risk analysis as "preprocessing" to scanning, which allows organizations to differentiate various classes of assets, she says.

Another trend is the emergence of "in

the cloud" scanning services. In addition, "established [vulnerability] scanning firms are and will be bolstering their Web application scanning capabilities," Roberts says. "Otherwise, features that ease reporting and management seem key. Integration with back-end user directories to make access to [scanning tools] easier and reports geared to compliance are much in demand."

Here are steps to take when evaluating, buying and deploying these products:

1. Consider a variety of factors, not just cost and scanning capabilities, when selecting products. Experts say it's wise to look at a number of key areas before investing in a scanning product.

"A lot of it depends on your organization and what your priorities are," Roberts says. "Is cost/affordability the most important thing to you [or] do you need something that can scale across a large network with thousands of endpoints? Is compliance your main driver here or is this part of a more general effort to improve your security posture? Do you have some larger policy store [that] this needs to integrate with or will this be a standalone operation? Are you Windows only or Windows plus Linux, Mac, Unix, etc.?"

When selecting a vendor and product, be sure to consider enterprise support and scalability, Wang says.

The Shift Toward Enterprise 2.0

WEB 2.0 TECHNOLOGIES BRING BENEFITS AND CHALLENGES TO THE ENTERPRISE, AND CSOS MUST MANAGE THIS TRANSFORMATION IN A SECURE AND EFFICIENT WAY.

> CSOs are both eager and cautious about bringing Web 2.0 tools into the enterprise and transitioning to an Enterprise 2.0 environment.

On the positive side, community-building networking applications and services can effectively link customers, suppliers, partners, and employees for fast and easy collaboration, which can quickly lead to greater productivity, effective data sharing, visibility into business processes, and ideally, improved profitability.

But on the flip side, Web 2.0 technologies come with myriad risks: business-inappropriate content or applications finding their way on to company computers; the increased possibility of viruses, worms, and malware; and accidental or malicious data loss.

Enterprises are still exploring the best uses of Web 2.0. **Corporate sales and marketing departments have taken the lead, using social applications to enhance customer relationships, attract new audiences, and heighten brand awareness.** For example, Dell offers a community network that provides communication forums, idea centers, blogs, and feeds that keep visitors informed, as well as provides opportunities to learn, participate, and collaborate.

Other organizational departments are taking advantage of Web 2.0 as well. For example, IT departments have created internal wikis and blogs to keep employees up-to-date with company information and allow for easy communication.

2.0 CHALLENGES

Even though Web 2.0 has many advantages, it still poses significant risks. The new network perimeter is no longer a building with walls and network cables, and securing it is becoming as difficult as defining it.

Users now demand anytime access from anywhere, using laptops, remote kiosks, and PDAs to access corporate information. So if you're sitting at a coffee shop accessing Webmail, communicating with friends, and updating your blog, are you inside or outside the company network?

Although most organizations have established standard protections such as e-mail filters, firewalls, and virus signatures, **the ingenuity of hackers means that viruses, worms, and malware take on new shapes and infiltrate in new ways.**

Furthermore, because many Web pages and sites can no longer be classified as simply "good" or "bad," reputation is becoming less reliable as an indicator of threat potential. For example, Google may be trustworthy in and of itself, but users who build their own iGoogle portals with content coming from non-Google sites are beyond the hosting site's control.

These challenges may lead some people to believe that Web 2.0 should be banned in the workplace. Realistically, this is nearly impossible. Due to the increasing use of mobile devices, cloud computing, software-as-a-service models, and customer portals, Enterprise 2.0 is inevitable.

The new approach is to say "Yes" to Web 2.0 as a way of empowering employees to be more technologically efficient, and encouraging the Employee 2.0 mentality. The trick is to combine Web 2.0 technologies with the appropriate security measures.

But how can you, as CSO, give employees all the functionality and rich experiences of Web 2.0 without opening the door to attacks, viruses or other threats?

Experts agree that a secure Web gateway can help you gain visibility and control of inbound and outbound Web traffic. Learn what to look for in a secure Web gateway by downloading *A Competitive Guide to Selecting Secure Web Gateways* now at www.websense.com/cso

>> TOOLBOX

Networks are likely to grow in terms of size and usage, and vulnerability scanning capability must be able to keep pace with that growth. Wang says other factors to consider when evaluating products include reporting capabilities, support for trending analysis and support for regulatory compliance.

Among the factors that German-based bank WestLB tested and evaluated before selecting a scanning product from eEye Digital Security were patch-level accuracy, operating system identification accuracy, scan performance and ability to check both file versions and registry. The bank then used a scorecard rating system to grade the products available, says Kenneth Pfeil, executive director and head of information security for the Americas region.

For County Bank in Fresno, Calif., ease of use was a major consideration. Among the questions the company asked before selecting a product from Qualys was how much work it would take to generate reports, how easy it is to customize reports and what the learning curve is for setting up the system.

"Some of these systems are great conceptually but they're so complex that the implementation never gets done," says Charles McClain, vice president of information security at County Bank. McClain says it's important to include the people who will be using the system in the product selection process. They can weigh in on what features might be most useful.

2. Analyze risk before analyzing network traffic. Prior to installing a vulnerability scanning system, security managers should conduct a thorough risk analysis to determine where they need to be most diligent when it comes to scanning.

Other steps to take before plunging ahead with scanning, Pfeil says, include being prepared to spend a significant amount of time getting everything running properly. Getting scans running and configured properly can take weeks.

Establish patch baselines, have scans coordinated around maintenance schedules and run small test scans on isolated systems on disparate subnets.

3. Be prepared for disruptions. "The thing to remember with [vulnerability] scanning is that it's an activity that potentially can touch and disrupt every corner of

your network," Roberts says.

The tendency is to fire up a scan and see what you find, Roberts says. "That is a bad idea for a whole bunch of reasons. First of all, vulnerability scanning is a high-bandwidth kind of activity that has the potential to bring areas of your network to [its] knees, if not carried out thoughtfully."

Also, some of the tests carried out by automated or manual vulnerability scans can create denial of service or "blue screen" conditions on network hosts, application servers and the like, Roberts says. It's a good idea to get input and buy-in not just from senior management but from the various network administrators, application administrators, help desk people, etc., Roberts says.

Solicit input from the various functional groups within your organization about issues such as the right times of day to carry out scans and which processes can't be interrupted.

4. Make sure you have the skills in place to leverage scanning technology. It's important to have inside experts to interpret scanning results, Wang says. "Many scanners yield many pages of results, and it takes experts days to go through the results," she says. "It is critical to have such expertise

in-house."

Even if you're the person or group that "owns" the vulnerability scanning function, "if you work at a company of any size, you probably don't have comprehensive knowledge of every nook and cranny on that network, what applications are running and when, what kind of data is being managed and so on," Roberts says.

5. Make scanning an ongoing activity. "Just starting a [vulnerability] scanning program in itself isn't going to solve your security problems or make your IT organization more efficient," Roberts says. "In fact, in the short term it's going to give you a lot of new data and responsibilities to manage."

Over time, companies might need to tweak and refine scans to get the reports they need. "The visibility [scanning] will give you into your network—what hosts are running, their relative value and what their security posture is—will make it much easier for you to assess the overall security of your organization and to design programs and processes to address real versus perceived problems." ■

Bob Violino is a freelance writer based in New York. Send feedback to Editor Derek Slater at dslater@cxo.com.

Who's Who

Major vulnerability scanning vendors, as identified by The 451 Group and Forrester Research:

Advanced Research
www.arc.com/corporate.shtml
Product: Security Auditor's Research Assistant (SARA)

Cenzic
www.cenzic.com
Product: Hailstorm Enterprise ARC

Cymtec Systems
www.cymtec.com
Product: Cymtec Sentry 2.0

eEye
www.eeye.com/html/index.html
Product: Retina Network Security Scanner

GFI
www.gfi.com
Product: Languard Network Security Scanner

Fortify Software
www.fortify.com
Product: Fortify 360

Infiltration Systems
www.infiltration-systems.com
Product: Infiltrator

ISS Internet Security Systems
www.iss.net
Product: Internet Scanner

Lumension Security
www.lumension.com/home.jsp
Product: PatchLink Scan

McAfee
www.mcafee.com/us
Product: VirusScan Plus

Microsoft
www.microsoft.com/en/us/default.aspx
Product: Microsoft Baseline Security Analyzer

Ncircle
www.ncircle.com
Product: PCI Scan Service

NScan
www.nscan.org
Product: NScan

OutPost24
www.outpost24.com
Product: OutScan

Perimeter eSecurity
www.perimeterusa.com
Product: Vulnerability Defense

Qualys
www.qualys.com/index.php
Product: QualysGuard

Rapid7
www.rapid7.com
Product: NeXpose

SAINT
www.saintcorporation.com
Product: SAINTmanager

StillSecure
www.stillsecure.com/index_flash.php
Product: VAM

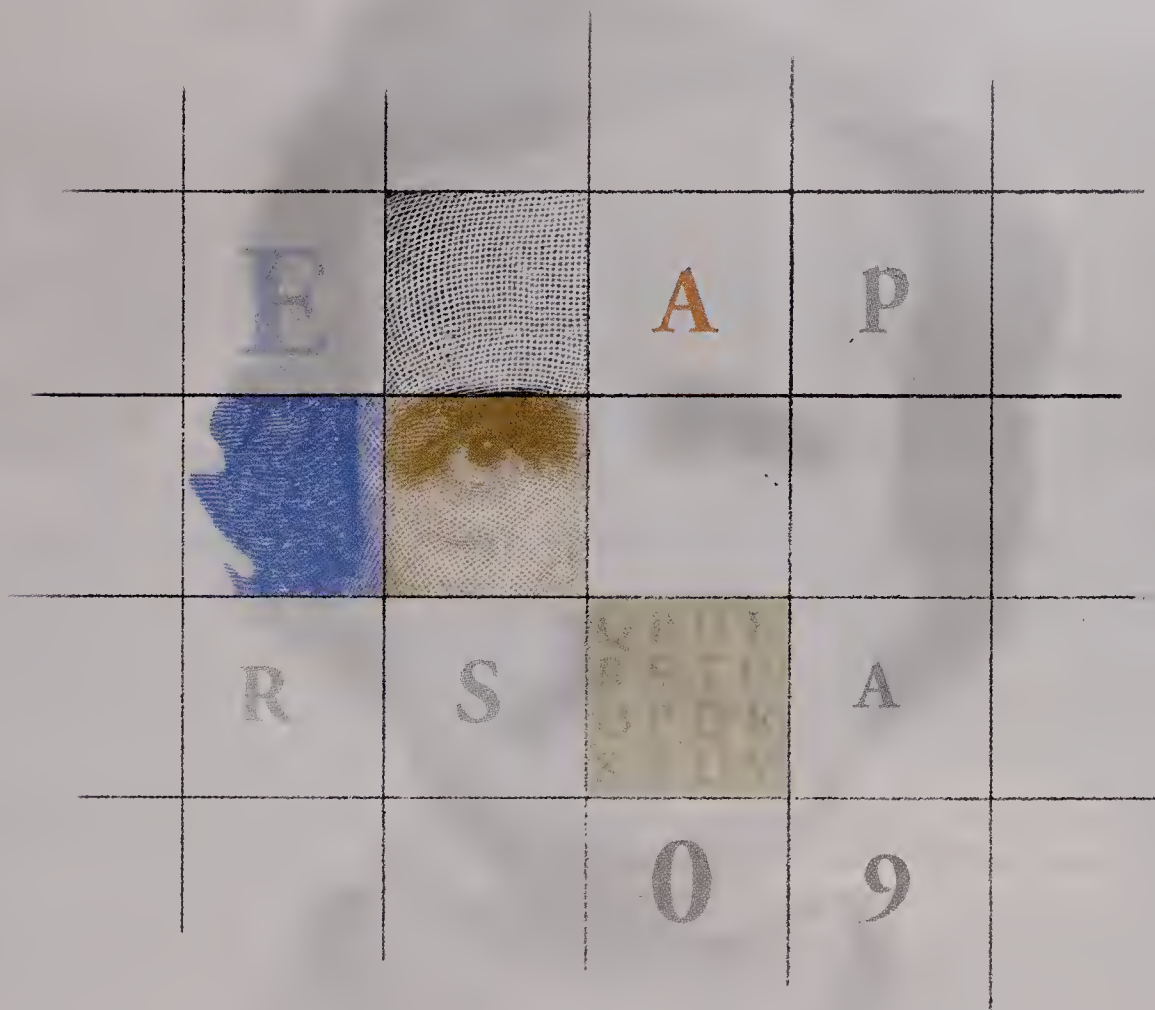
Tenable Network Security
www.nessus.org/nessus
Product: Nessus Vulnerability Scanner

RSA[®]CONFERENCE

WHERE THE WORLD **TALKS SECURITY**

When the next security threat hits, be ready to hit back.

U.S. businesses lost an average of \$289,000 in 2008 to security breaches.[†] No business or organization can afford exposure to that kind of risk. Educating yourself on the strategies and solutions you need to stop this exposure is your imperative. RSA[®] Conference is the one place where you can meet with experts, colleagues and vendors to find solutions that will positively impact your information security programs now and in the future. It's a security investment you can count on to deliver results — and it's all at RSA[®] Conference 2009.



REGISTER NOW

APRIL 20–24, 2009 | MOSCONE CENTER | SAN FRANCISCO
WWW.RSACONFERENCE.COM/2009/CSO
ENTER PRIORITY CODE: CS039

[†]Computer Security International (CSI) Computer Crime and Security Survey, 2008.

Right on Time?

Every computer in your company has a clock. Forensics demands precise synchronization. Do you have the time?

BY SIMSON GARFINKEL

IS THE CLOCK on every computer system in your organization set to the correct time? If your answer is no, you're not alone. According to a 2007 study by Florian Buchholz and Brett Tjaden, both professors at James Madison University in Virginia, more than a quarter of the Web servers on the Internet have their clocks off by more than 10 seconds.

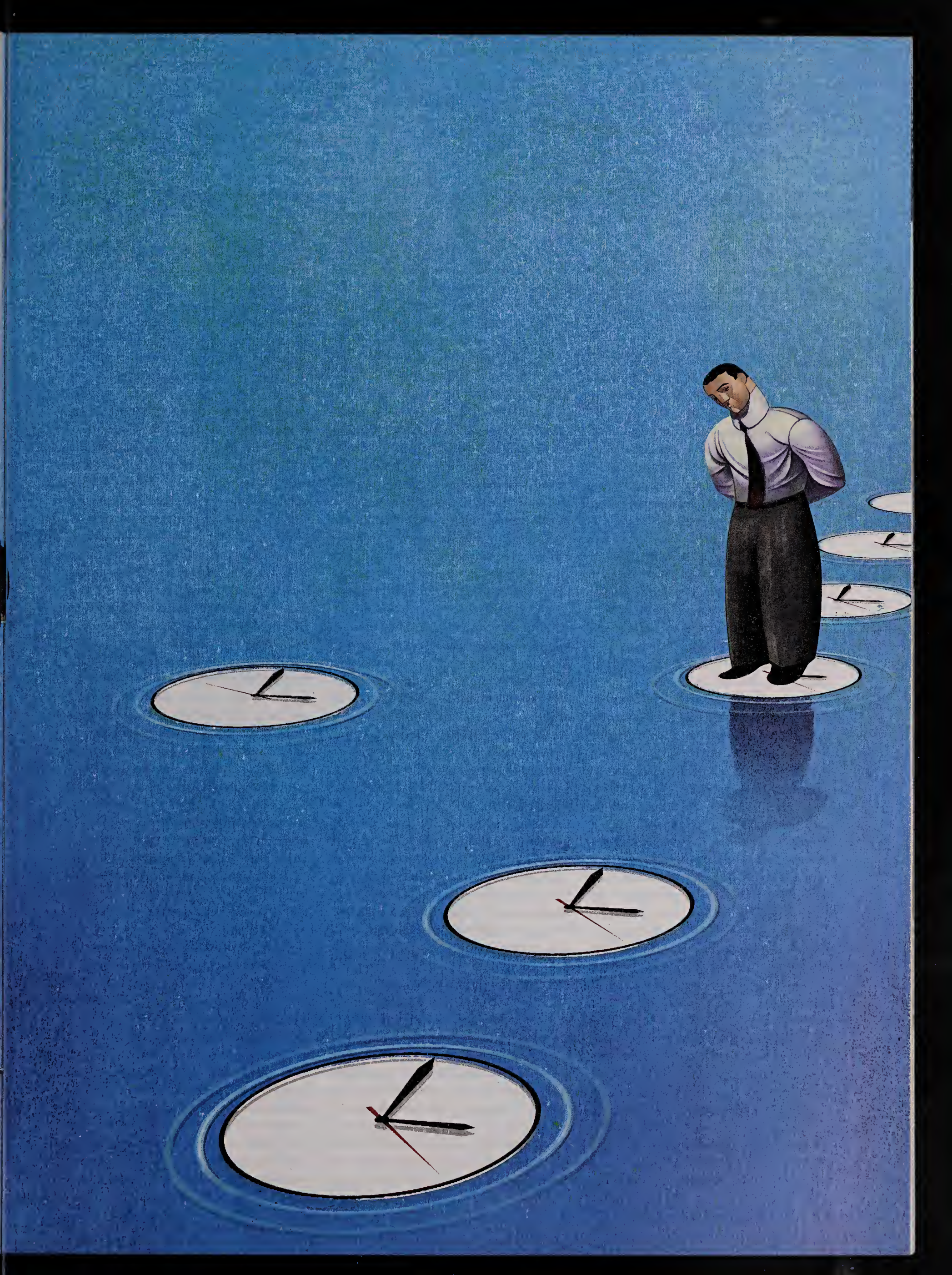
Making sure that computers are set with the correct time is one of those seemingly petty technical things that can unfortunately have big, negative consequences if not done properly. That's because assumptions about time and its flow permeate modern

computer systems—including software, hardware and networking. This is true of desktop systems, servers, mobile devices and even embedded systems like HVAC, alarm systems and electronic doorknobs.

Buchholz and Tjaden studied Web servers because they are particularly amenable to analysis: Every time you request a page from a modern Web server, the server sends back an HTTP header called "date" which indicates the time-of-day for the server's clock. But unless your organization has made an effort to keep time in a precise and accurate way, the chances are very good that you're doing a bad job.

Does Your Server Have the Time?

Having the correct time is important for security because system clocks are used for a lot more than just displaying the current time on your organization's homepage. Web servers write the time of every page downloaded into their log files: If the time-of-day clock is wrong, the log files are also wrong. This can be a problem if you are trying to figure out an attack that originated inside your organization. You may want to correlate file accesses with whether or not a suspect was seen at a desk, in a meeting or was known to be out of the office. But it's



also important for attacks that originate outside your organization. That's because many attackers will mount their attacks from dynamically assigned IP addresses; if your time is off by a few minutes (or more), it may be nearly impossible to figure out where the attack came from or who was responsible.

Log files are just the beginning. Every time a file is modified, accessed or has its metadata changed, modern computer systems will update the file's so-called "MAC times." Forensic tools like EnCase, FTK and Sleuth Kit have the ability to read all of the MAC times within a computer system and sort them to create a single time line. Incident response teams will typically use these time lines to figure out which files an intruder browsed or modified.

Because clocks are so often set incorrectly, some forensic tools will allow the security practitioner to enter a time offset or "delta" when a log file is constructed. But these tools assume that a computer's time offset is constant—that if the computer was 30 minutes slow today, it was also 30 minutes slow three months ago. Unfortunately, that assumption isn't valid.

During their six-month study of more than 8,000 Web servers, Buchholz and Tjaden found that systems with the wrong time frequently drifted—or jumped—in unpredictable ways. Some systems would get steadily slower or faster, and then jump back to the correct time. Other systems were rock solid in the rate that time passed, but they were off from the correct time by minutes, hours, days or even years. Some systems followed the wrong rules for Daylight Savings Time. And some servers appeared to have multiple wrong times—that is, one query to the server would return one time offset, and other query would return a completely different time offset, and then subsequent queries would alternate between the two. (The authors hypothesized that these situations happened when two or more physical machines with different time offsets were hiding behind a single IP address through some kind of load-balancing arrangement.) You can read the entire article www.dfrws.org/2007/proceedings/p31-buchholz.pdf.

The system's clock is used by many other processes and systems on a typical server. Since many tasks on a server are

keyed to the time of day, a server whose time is wrong or erratic may not perform automatic routine maintenance like accounting, scheduled cleaning of temporary files or rebuilding of system databases. Backups may not be performed or they may be inaccurate. Security patches may not be properly applied, automatic update scripts may not properly run. If the time is wrong, the entire server is potentially suspect.

Client Time

Getting the time right on your clients is important too—and not just so that security patches get properly installed. The SSL security protocol, the basis of secure Web browser and mail downloading, requires that your client knows the correct time. That's because SSL is based on X.509 public key cryptography certificates, and every SSL certificate has two time and date stamps inside—when the certificate starts being valid and when the certificate expires.

Time shows up in many other desktop applications. Many calendar programs display the current date in a different color and have a button that moves the calendar's display to "today." Many mail clients will change the way that date of incoming mail is displayed depending on whether the message was received today, yesterday or some other day in the past. These features won't work properly if time isn't set right.

Many e-mail clients automatically classify messages "from the future" as spam; spammers may set the date header in their message to be hours, days or weeks in the future in order to make their spam messages appear at the top of the user's mailbox. So if your computer's clock is in the past, it may think that every message it receives is spam.

Many standalone devices also have a built-in clock, which are frequently wrong as well. Setback thermostats that have the wrong time may make you inappropriately hot or cold. Recently, I had to consider the log of an electronic door lock to figure out who had entered a room—and when. The log took a lot longer to parse than it should have because it was off by an hour and 15 minutes and because it didn't adjust itself automatically when Daylight Savings Time rolled around.

How to Get the Time?

Getting and keeping accurate time actually requires two independent operations. First, the computer needs to have some way of knowing a precise point or mark in time; second, the computer needs to be able to adjust the frequency or drift of its clock to stay in sync with some presumably more accurate external source. Fortunately, having accurate time is so important that Windows, MacOS, Linux, PalmOS and practically every other modern operating system has built-in support for the Internet Network Time Protocol (NTP), which performs both of these features automatically.

But even though support for NTP is widely deployed, many systems have it disabled. Worse, few systems will alert when NTP is turned off. And worse still, the systems won't alert when their clocks are obviously wrong, even though such an alert would be an easy thing to do. While working on this article I checked NTP on five Macs, two PCs and a Linux system: Only one Mac and one PC had NTP enabled. The other systems were off by minutes, although the Linux server was off by more than two hours. Whoops.

When it's working properly, the NTP system should perform two related functions. When the computer boots it should ask a remote "time server" for the current time and set the computer's clock accordingly. And once the system is running, NTP should periodically monitor the remote time server and gently slow down or speed up the computer's clock so that it stays accurate and so that there are no sudden jumps in apparent passage of system time. (At least this is the way that it is supposed to work in practice. Some implementations crassly reset the system's clock to the reference clock. I've seen this cause problems with applications like Palm's desktop calendar.)

Microsoft and Apple both operate their own time servers and the names of these time servers are built in to their respective operating systems. MacOS, for example, will use the sever "time.apple.com" in North America. Many universities and businesses operate their own time servers as well: Using a local server can both give you more accurate time (because there is less network delay) and can cut down on network traffic from your organization. If you want to run a local time server, you can get the time

Ironically, most of the time servers on the Internet get their time from...other time servers.

from one of the public NTP servers operated by the NTP Pool Project (www.pool.ntp.org). In January 2009, there were more than 1,734 public servers operated around the globe, mostly in Europe and the U.S. There are detailed instructions on the website for configuring most operating systems to have accurate time.

Ironically, most of the time servers on the Internet get their time from other time servers. But NTP also has support for so-called "stratum-0" time devices, which get their time reference from one of the agreed-upon time standards. These stratum-0 devices connect to stratum-1 servers on the Internet. Servers that get their time from stratum-1 servers are called stratum-2 servers, and so on. When I wrote this article, "time.apple.com" was actually four separate stratum-2 servers, which presumably connect to other stratum-1 servers inside Apple.

If you are paying attention closely, something about the previous paragraph should have troubled you—that bit about "agreed-upon time standards," with emphasis on the plural. Although it seems like there should only be one time standard, sadly there are multiple ones. The official U.S. time is operated collaboratively by the Time and Frequency division of the National Institute of Standards and Technology and the Time Service Department U.S. Naval Observatory. Both of those organizations operate their own highly accurate clocks and compare them once a week; the two clocks are typically within 20 nanoseconds of each other, which is good enough for most applications. The time is available on the Internet, the telephone system and transmitted on three radio stations (WWVB, WWV and WWVH). If you have one of those clocks that sets itself by the radio (or by an "atomic clock"), it's probably listening to WWVB. U.S. Government time

is contributed to UTC time, also known as Coordinated Universal Time, GMT (Greenwich Mean Time) or Zulu time.

But there are other time systems out there. For example, there are many low-cost GPS receivers available that will provide the time to your computer. There are also cellular receivers that will pick up the time from Sprint or Verizon, since the CDMA telephone system that those companies use requires accurate time as well. Unfortunately, each of these systems is slightly out of sync with each other, but in practice, this really won't affect you most of the time. (Several years ago I noticed that Sprint's CDMA system in Boston was transmitting a time that was precisely five hours off; it looked like somebody had not properly set the time zone offset. The problem wasn't corrected for several hours.)

Leap Seconds

There is one more geeky little wrinkle in time that might affect you, though, and that is the handling of leap seconds. Recall that leap seconds are added because the Earth's rotation is slowing down due to the frictional action of the tides; the Earth hasn't had 86,400 seconds in a day (the old conventional measure) for more than a hundred years now. To deal with this unfortunate circumstance, the International Earth Rotation and Reference Systems Service, a group also known as the Time Lords, add a "leap second" every now and then to keep the meteorological day in sync with the day that our computer systems all use. We just had a leap second this past December. The standard way that computers handle leap seconds is to have the clock go to 23:59:60 GMT before they go to 00:00:00 on January 1st. (In New York City the leap second actually happened at 18:59:60 EST on December 31st.)

Leap seconds can cause problems because even though NTP and the lowest layers of most modern operating systems know that seconds sometimes go from 0 to 60 (and not their normal 0 to 59), few programmers are really up on all of the ins and outs of proper time keeping.

This past December, systems running Oracle Cluster Ready Services (CRS) clusterware crashed at 23:59:60 GMT, unable to handle the leap second that bubbled up from the operating system's underlying time service. Some Linux systems from Slackware, Debian and Red Hat also hung, apparently because of an underlying kernel bug. (This is unrelated to the bug that caused some Microsoft Zune players to crash on January 1st, 2009. That bug had to do with the fact that 2009 is not a leap year.)

Hopefully your good-natured response to this article will be to check and make sure that all of the computer systems in your organization have the correct time—and if they don't, add proper time keeping to the list of responsibilities for your security staff. Certainly having dependable time is important for good security, but it also makes other kinds of routine tasks like diagnosing e-mail delays and outages easier.

Ultimately, time is a security matter. Having correct time can be the difference between having someone convicted of a crime and having them go free. Indeed, if your system clock is wrong, you might not even know that a crime has taken place. ■

Simson Garfinkel is an associate professor at the Naval Postgraduate School in Monterey, Calif., and an associate of the School of Engineering and Applied Sciences at Harvard University. The views and opinions expressed in this document represent those of the author and do not necessarily reflect those of the U.S. Government or the Department of Defense.

G R O W T H

STRUCTURE

change

Priorities

Satisfaction

Strategy

TOOLS

AWARENESS

PLAN *to* SUCCEED

Excerpt: Identifying business goals and driving change are the keys to security strategy

BY TIMOTHY GILES

Creating a strategic plan for physical security requires much more than a knowledge of the tools. In his new book, *How to Develop and Implement a Security Master Plan* (CRC Press), former IBM Director of Security Timothy Giles lays out ideas for understanding business priorities and creating a security organization to match.

Before you begin the process of defining or redefining the security organization's strategies, you must first gain an understanding of the strategies of their business. You do this by interviewing the appropriate executives of the company: the CFO, COO and so on.

You need to know for the next five years:

What growth do they anticipate? Do they expect any product or service changes? Is the expansion or reduction limited to the existing facilities or will new ones be added? Do they expect any overseas expansions or mergers? Are there any

PHYSICAL SECURITY

major layoffs or outsourcing activities planned?

Some of this information will be considered to be highly confidential, especially any mergers or layoff activity, but you need to understand these directional moves if you are to plan how they will deal with them from a security standpoint. It is not necessary for you to know all of the details. For example, you don't need to know who they plan to merge with or to whom they plan to outsource work. Yet you'll need to know what countries are involved if your client will have any stake or ownership in the relationship. If the person performing this master plan activity is an outside consultant, the executives may prefer to only share this information with the in-house director of security or chief security officer. If there is no in-house staff, the consultant will need to discover as much of this information as possible and may need to sign a confidential disclosure agreement (CDA). (I believe a CDA should always be part of the contract with the consultant.)

The security organization's strategies deal with all aspects of the program from policies and procedures to technology and staffing. Their strategies should be docu-

mented so they reflect where they are now and where they're going. I believe strongly in the saying, "If you don't know where you are going, you won't like where you are when you arrive!" In order to implement new security strategies, CSOs or directors of security should first address the process of change. They would prefer everything stay as it is. So the question the CSOs should be asking of themselves is this: Is change a friend or foe? The answer to this is quite simple: It's up to them! Change is a topic that is discussed continuously in the business world. But, as the adage says, talk is cheap!

As an example of implementing change, I would cite the most dramatic project that I have undertaken in my career. If you have not personally been involved in a major change effort, then perhaps my experience can help you to understand the complexities of this effort. As a part of the reengineering effort in IBM, we reorganized the internal security operation in September of 1994. We took the security professionals who were managed site-by-site by nonsecurity personnel and brought them into one single structure, managed by security professionals. However,

this did not in and of itself make change happen. What it did do was to provide the opportunity for constructive, consistent and rapid change.

Over the next two years, we reduced costs by approximately 30 percent, we increased customer satisfaction to 94 percent and we significantly increased our own security employees' morale. In September of 1997, I was awarded the Security Director of the Year recognition by *Access Control & System Integration* magazine. As people passed on their congratulations to me, I explained that I take credit for primarily one thing, and that is creating the environment where "change" is a "friendly" activity. The accomplishments of our organization are directly attributed to our own people embracing the concept of change and making it happen.

So exactly what did we do to create this environment? Basically, we did three things:

First, we implemented the use of project teams on as many different aspects of our security business as we could think of. These teams had two goals to accomplish: Find the best internal or external practice for the specific area they are looking at and—even more important—

increase open communications across the organization. Second, we implemented a measurement program to find the defects in our processes. To make this successful, I declared this to be a "no fault" measurement program. The primary failure in this program would be if you did not find problems. The secondary failure would be if we did not fix the problem. Third, we launched a massive campaign to do national contracts and centralized systems to eliminate as many redundancies and inefficiencies as possible. All of this combined translated into massive change for our people and our strategies in the way we implemented security.

We knew that the only way we could be successful was for our people to see this as something that would be good for each and every one of them, personally. To make this happen we first had to convince them that change was absolutely necessary to the survival of IBM and our jobs. You might think this would be obvious to all of us considering our company's financial performance over the early 1990s, but some people have a way of convincing themselves that they are not part of the problem. Therefore, what we had to do was to convince them that change had to happen, and we had two choices:

- Deny the need, resist the change, and FAIL, or...
- Embrace the need to change and DRIVE that change.

If we, the security professionals, truly and fully accepted this, we had the power to decide our future. If we did not drive change in our organization, someone else would, and we would have much less control over the outcome.

One of the primary tools that we provided to our project teams to do their analysis was the implementation of an internal benchmarking program followed up with a detailed resource and task analysis program.



After implementing many of the changes and realizing the benefits, we then launched an external benchmarking effort. This data demonstrated that, when compared to any other companies, we were significantly more cost competitive.

As any good business manager can tell you, the best resources of any company are its employees. I personally believe that this group of security professionals is the best, but I acknowledge that I might be slightly biased on this point. However, the proof is in the results. It is important to remember that change is not something that you do and you are finished. Instead, it is an ongoing process

- should be involved in the decision to use them;
- ■ Use of a polygraph for interrogations;
- ■ Whether or not to prosecute employees or others when a crime has been committed (even a minor crime).

TECHNOLOGY

- ■ What technologies might be utilized in the future and when, where and why?
- ■ What is the migration plan for moving to the new technologies?
- ■ What is the anticipated end of life of the current technologies in use?

OVER THE NEXT TWO YEARS, WE REDUCED COSTS BY APPROXIMATELY 30 PERCENT, WE INCREASED CUSTOMER SATISFACTION TO 94 PERCENT, AND WE SIGNIFICANTLY INCREASED OUR OWN SECURITY EMPLOYEES' MORALE.

that must be continually driven from senior management down through the organization and by the employees up through the company. This is why it is essential that you create the right environment for change to flourish.

A critical part of that environment is your own attitude. Your employees will know very quickly if you are just giving lip service to this process or if you are serious. Just as the scenery changes as you travel down a road, your business and even you and your employees must be in a continuum of change. If you are, you will not just succeed, but you will have ongoing success. It is this environment that makes it very important that you have documented, long-term strategies and that you reevaluate those strategies on a regular basis. After all, that is the map you will be using for your trip.

So, what are your client's strategies? As I said earlier, they should cover all aspects of their programs. It would be very difficult for me to suggest any generic strategies because there are many variations depending on the business they are in. As you develop them, you should utilize the functional team, the stakeholders that I spoke about earlier, to assist. Here are some examples of the areas that should be addressed:

POLICIES

- Education and awareness programs;
- Badge wearing;
- Clean desk policy;
- Visitor and contractor controls;
- Employee involvement and responsibilities;
- When and how to have armed off-duty police officers onsite.

INVESTIGATIONS

- Use of hidden cameras along with determining who

- Developing a replacement schedule for existing equipment.

STAFFING

- The use of armed or unarmed security officers documented with the reasoning for the decision;
- Which positions can or cannot be contracted, regardless of whether they currently are or are not contracted?
- What style of uniforms should be worn and why?

As you go through the process of helping them in documenting their strategies, they will find that they are already following several strategic lines—they just may not have documented all of them before. A good example of this is the use of unarmed security officers. I personally do not like to have armed security people onsite except in rare applications such as a nuclear plant or a top-secret installation. Obviously, many CSOs or directors of security feel the same way because the majority of businesses in the United States use unarmed officers. However:

- How many of these security managers or businesses have documented that decision to demonstrate it was a well-conceived strategic decision?
- Was executive management involved in, or at least apprised of, the reasoning for this decision?
- If a workplace violence shooting were to occur onsite, would they be prepared to defend their decision of unarmed officers in court?

Having these strategies well documented can be invaluable in situations of litigation or even when a decision about an unusual situation has to be made in a timely manner. Their documented strategies should always be their guide. ■

[UNDERCOVER]

By Anonymous

The Company that Did Everything Wrong, Part II

The conclusion to last month's tale of a comical yet sad visit to a company that suffered a data breach

It was 1 a.m. and we had been working on our client's data breach for eight hours. Most of the team had been awake for 20-plus hours, and fatigue was starting to set in when Bob discovered something.

He realized that a piece of malware that was embedded in the phishing attack linked back to a website in Spain. "I did a little research and that site in Spain is a compromised host," Bob told me. "These attackers are very clever. They mirrored the normal landing site with one that they set up that contains their exploits."

"So instead of a visitor landing on the regular home page, they land on a compromised, hidden page?" Sam asked.

"Correct," Bob said. "This has the hallmarks of an extremely sophisticated attack."

Bob has a lot of credibility in my book, so when he talks about sophisticated attacks, I take notice.

"Why do you say sophisticated?" I asked.

"First, there's the malware package. Looks like its polymorphic, changes its digital signature at every execution. So creating a digital hash won't help us locate other infections," Bob said. "Of course I won't know for sure until we have a chance to send it to Dave for him to decompile, but I have a pretty good feeling that it is. Then there is the amount of research that had to go into crafting the phishing e-mail. It uses all the right buzz words, talks about a current

project and even lists company employees who aren't listed on the company's website. Then there's the amount of effort they took to hide their site. Take a look at the homepage for this site." Bob turned his laptop around so everyone at the conference table could see the screen. "Here is the regular site: www.compromisedsite.com/index.html. But here is the link for the site that contains the exploit: www.compromisedsite.com/index.html. See the difference?"

"They look the same to me," said Sam.

"They did to me, too. For a long time. But

compromised site using one of our sand boxes?" I asked him.

"I did just a couple minutes ago. The results are very preliminary, but I think they confirm the fact that this is a well-planned attack. The site tries no less than five different browser attacks, and that's if the user doesn't click any of the links! I don't know yet how many attacks the links launch. Also, the Spanish site seems like it might be a site that some employees of the client would need to access for normal business operations. That would explain why it

was so important for the attackers to hide their presence on that server."

Armed with that information, Sam and I met Victor, our Russian colleague, down in the server room. "Hey boss! Welcome to ze dungeon data center. Ha-ha! Guess vat I have found?" he asked.

"Tell me you have good news, Victor," I said.

"Vell boss, ze system administrators turned off all ze logging. No more of doze damn alerts going

off! But zey did not turn off everything. And I found vat zey did not! Look here."

Victor showed me the log file index of the company's antivirus software. "See how ze log files are small here, and here and here, too," Victor points to the logs from Tuesday, Wednesday and Thursday of the previous week. "But look here. Friday ze log is four times bigger than for ze other days of ze week. I tink somezing happened on Friday. And ven ve look here, ve see this IP address



here's the difference: The uncompromised site has a regular Times New Roman letter *i* in the name: index.html. The compromised landing page uses the special character *í*—an accented *i*."

It's tough to notice, and of course that's the point. Whoever compromised this site went to a lot of trouble to hide the fact from the Web owner, and even from fairly savvy computer users, Bob said.

"Did you have a chance to connect to the



Lose the
free donuts
on Fridays.

© 2009 Fortify Software Inc.

Some things can be sacrificed, but your cyber security isn't one of them. It's a matter of survival. And if you're just protecting your sensitive data at the network perimeter, we've got news for you—your software is seriously vulnerable and you need help. Fast. Fortify delivers the only preventative approach to software security. Reducing the risk of catastrophe from cyber attacks and helping you meet tough compliance mandates. Don't wait another second, contact us at 650-358-5600. After all, when it comes to your security who can afford to take a coffee break anyway?



fortify.com

over and over and over and over. It's an IP address from ze Russian Federation. Telephone company in St. Petersburg."

He suggested we wait an hour and come back. St. Petersburg is at lunch time now but he said he'll call them in an hour and see what information he can get.

Back in the conference room Michael was sitting at the table talking on his BlackBerry. He was looking pretty ragged, his eyes bloodshot and a new coffee stain on his shirt.

"I'll tell them. Right. Bye," Michael said as he finished the phone call. "That was

"Russian people understand authority. Sometimes you have to make them believe dat you are ze authority. Dats vie I was little animated in ze phone call. Ha-ha-ha! Russian hackers compromised ze e-mail server some day earlier than last Friday. Ve don't know ven ze original compromise happened, but ze computer vas used for demonstration at ze hacker convention Friday last week," Victor said.

At that point, Bob approached me. "Eamon, can we talk in private for a minute?"

Alone in Michael's office, Bob picked

ing demonstration at a convention in St. Petersburg;

- On Monday of this week, an employee clicked a link in a phishing e-mail. This e-mail contained information about the company and a project that they are currently working on, so this attacker either had insider knowledge or did quite a bit of research about the company;
- All of the data from a different employee's hard drive (not the one who clicked the link) was seen traversing an Internet link monitored by the Air

"Hey man, your guy is down in the server room actin' all crazy. He's yellin' some kinda gibberish on his cell and getting all red in the face. You better take a look at him before he **busts a vein** or something."

the CIO. He wants us to brief him before we make our presentation to the CEO and the board."

"We're making a presentation to the CEO and Board?"

"Oh yeah, sorry. Forgot to tell you. Tomorrow morning. Well, actually this morning at 7."

Not much time to prepare anything since it was already 5:45 p.m.

A short time later, the systems admin who had been working with Victor burst into the conference room and said, "Hey man, your guy is down in the server room actin' all crazy. He's yellin' some kinda gibberish on his cell and getting all red in the face. You better take a look at him before he busts a vein or something."

As if on queue, Victor threw open the near door of the conference room and came in. "I have information about ze group dat used dat server as demo platform for hacker convention," he said. "Ze IP address that vaz in ze antivirus logs vaz registered to dis vireless telephone company. Dey told me dat dey rented this IP range to ze hacker convention. So ve have proof dat dis group attacked ze e-mail server earlier, because vie would dey use a server dat was not already compromised? Dey don't! Dis server vas compromised before!"

"Wow! Were you on the phone to Russia?" I asked. "Is that why the sys admin thinks you were yelling?"

up the phone and started dialing. He must have hit at least 30 keys before he put the headset to his ear.

"Tremendous Fury. Yes that's right, Tremendous Fury. This is an insecure line. Yes," Bob started spelling the name of the client using the NATO phonetic alphabet (Alpha, Bravo, Charlie, etc.). "I'll look for an e-mail." Bob hung up. "I have to wait for an e-mail but I don't think the Russians are the culprits here, or at least not the cause for the call from the Air Force OSI. This thing just doesn't have the feel of a Russian hack, at least as far as the phishing attack goes. I respect Victor and believe in what he found, but I don't think that the phishing attack was Russian in origin. Maybe this box was compromised twice."

"That's a bombshell," I said. "I'm going to wait before I hit that alarm bell. Maybe later on in the investigation we'll have confirmation."

Back in the conference room the entire team was there, including Michael, and we all had fresh coffee.

Ten minutes until the meeting with the CIO.

Here's what I wrote down:

- The company's e-mail server was compromised on date unknown but earlier than last Friday;
- This server was used by a Russian hacking group last Friday;
- This group used the server for a hack-

Force OSI;

- A call from the OSI alerted the client to the fact that they had been compromised. The organization did not detect this themselves due to insufficient security controls;
- The malware from the phishing attack has an IP address hard coded into it which links to a compromised Web server in Spain;
- We know the attackers are on the network, probably even this minute, because they orchestrated the removal of 120GB of data from the above hard drive. "Have I missed anything?" I asked. "China. I just received an e-mail from a friend." Bob said.

"That's a bombshell," I said. "OK, then. Let me change this."

We are dealing with at least two attacks. The e-mail server was compromised by a Russian group and the phishing attack is Chinese.

How we would come to wish that the client had been compromised by only two groups. In the next few days, the team would make discoveries that risked national security and would culminate in the resignation of the CIO. ■

The author leads a Computer Incident Response team. He may be reached at the pseudonymous amonmadreen@gmail.com or eamonmadreen@hushmail.com.

"I am fearless.

I am CSO for a major
manufacturing company.

I protect more than
intellectual property and plans.

I secure our reputation.

I know confidence
drives innovation.

I am fearless."

#1
In Vendor Value
2008 CIO Insight Vendor Value Survey



Secure Enterprise Data. Information is your company's greatest asset. The accidental loss, manipulation or theft of data is your greatest risk. RSA can help minimize that risk with data loss prevention solutions that secure sensitive data across your entire IT infrastructure.

Because the more confident you are in your data, the more confident your customers are in you.

Don't just secure your business. Accelerate it. Learn more at www.rsa.com/windsurf/cso

Visit us at the RSA Conference, April 20-24, 2009, San Francisco CA



The Security Division of EMC

Secure Anytime
Anywhere Access

Protect
Customer Identities

Secure
Enterprise Data

Manage Compliance
and Security Information

[INDUSTRY VIEW]

By Tom Reilly

Employee Monitoring: Good for the Employee?

ArcSight's CEO argues that "Big Brother" concerns are misplaced

Ever since the advent of the first business, trusted employees have stolen from their employers. Occasionally they stole for revenge or even excitement, but for the most part, they stole for money. Traditionally, perpetrators have been found in the stock room, maybe working a register, or handling accounting. However, with the advent of corporate IT networks that provide hundreds of thousands of employees with easy access to highly valuable information, the most dangerous of perpetrators are now sitting in a cubicle row or in a corner office.

A quick scan of headlines reveals that these perpetrators are of both genders and are found in all geographies and industries.

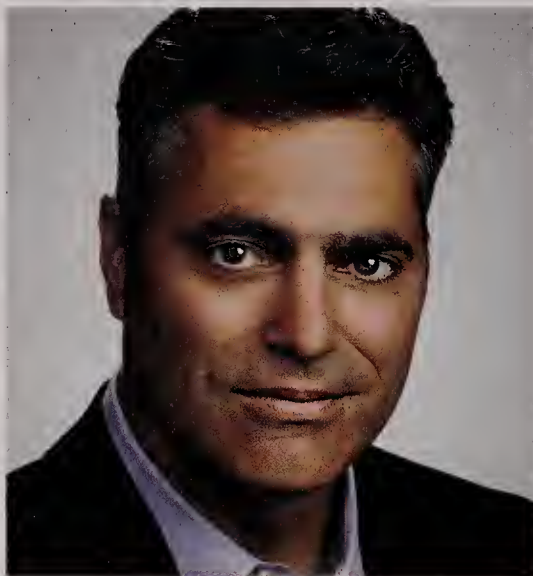
- A Dupont scientist stole \$400 million in intellectual property from his employer in the form of 16,706 documents and over 22,000 scientific abstracts.
- An employee working in a Texas physician's office that was contracted to treat FBI agents attempted to sell an agent's health records to drug traffickers for \$500.
- A Federal Emergency Management Agency employee stole the identity information of 200 people and opened \$150,000 in credit accounts.

Unfortunately, with the recent economic downturn, more white-collar workers might feel that the reward or the vengeance of stealing from their employer may outweigh the risk of being caught. Job losses, plummeting 401Ks, foreclosures and fire-sale mergers are taking a financial toll on the best of workers who feel they have no control over their destiny.

Combine increasing financial stress with easy access to highly valuable corpo-

rate data and a multitude of online black market outlets that turn information into cash, and you have the perfect recipe for insider cybercrime.

Never before have so many employees had so much access to such a wealth of data. For example, an employee with access to sensitive information doesn't have to be a world-class hacker to print it, copy it to an



MP3 player or e-mail it to a friend. Knowing this, many organizations have already increased their vigilance by monitoring activities that may signal insider threats:

- What applications are employees using and how are they being used? What data is being accessed and how much? What information is being downloaded, printed or e-mailed, and at what time of day?

When we work as security advisors to our customers, we are increasingly asked for tools and processes to better monitor how trusted users such as employees, consultants, partners and others are operating on the network.

Our clients have clearly shifted from

worrying mostly about external hackers, worms or phishing attacks to worrying about the insider threat, which now appears to be their number-one concern. Based on what we're seeing globally, there will be a greater onus on monitoring for insider activity and determining the "who" when an incident occurs. Questions such as who did it; should they be doing it, and if not, what else are they doing; how long has it been happening; and who else is involved, need to be addressed efficiently and effectively. At the end of the day, you can't arrest a laptop.

Some people might see this as "Big Brother." Perhaps surprisingly, not only are organizations pushing for this type of monitoring, but so are many employees. In these hard times, an attack on a company could have a direct impact on employees; the company could even go out of business and employees could be out of a job. This is exactly what happened to Ellery Systems in Colorado when an employee gave intellectual property to a competitor. This case helped lead to the Economic Espionage Act of 1996, which makes the theft or misappropriation of a trade secret a federal crime. Since the damage caused by an insider can be substantially higher than that caused by an outsider, prudence dictates that insider monitoring be put in place for everyone's protection. Much like a store owner keeps an eye on his inventory and registers, corporations are keeping an eye on their most important asset: information.

Monitoring for malicious insiders isn't "Big Brother." It's smart business and it helps protect employers as well as their employees. ■

Tom Reilly is president and CEO of ArcSight.

Striking the balance



CSO Perspectives

**Thank you to our
event sponsors:**

Platinum Sponsors

PRICEWATERHOUSECOOPERS 

websense
ESSENTIAL INFORMATION PROTECTION™

Gold Sponsors

 **CORE**
SECURITY TECHNOLOGIES

 **protegrity**

Silver Sponsors

ArcSight 

RSA
The Security Division of EMC

 **symantec.**

TDS
SECUREZONE

 **TREND**
MICRO

 **verizon**business
Security Solutions powered by Cybertrust

Emerging Solutions

Agilysys..

 **Archer**
technologies

 **CENZIC**
Securing Enterprise Applications

 **Lumension**
IT Secured. Success Optimized.

Visit:

www.CSOonline.com/events

for a complete listing of all CSO magazine
events

CSO
BUSINESS RISK LEADERSHIP

[DEBRIEFING]

Chicken Run



Security showed its marketing value once again in February as Yum Brands trumpeted the return of the exiled KFC secret recipe to newly fortified storage. The new digs feature a two-foot-thick concrete ceiling and floor and motion sensors.

Previously, company officials said, the recipe was kept in a filing cabinet.



**Compliance is tough
unless you are prepared
for what is coming.**

Tenable Network Security provides a suite of solutions that provide real-time compliance monitoring. Because networks are constantly changing, monitoring your network in real-time not only helps you know that you are ready for the next external audit but also gives you greater situational awareness of your overall security.

www.tenablesecurity.com/solutions

**Visit us at the RSA Conference 2009
April 20-24 in San Francisco
Booth 756**



TENABLE

Network Security®

**YOU DON'T
NEED MORE
SECURITY.
YOU NEED
BETTER
SECURITY.**



CA Security Management software streamlines your IT security environment so your business can be more secure, agile and compliant without upsizing your infrastructure. All with faster time to value. Greater efficiency starts with more efficient IT. **THAT'S THE POWER OF LEAN.**

Learn more at ca.com/security

Copyright © 2009 CA. All rights reserved.

